UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

REBECCA TUTEUR, ANTHONY VITI, and MATTHEW NAPOLI, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

METROPOLITAN OPERA ASSOCIATION, INC.,

Defendant.

Case No. 1:23-cv-03997-KPF

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Plaintiffs Rebecca Tuteur, Anthony Viti, and Matthew Napoli (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated, allege the following Class Action Complaint (the "Action") against the above-captioned Defendant, Metropolitan Opera Association, Inc. ("Defendant" or "The Met") upon personal knowledge as to themselves and their own actions, and upon information and belief, including the investigation of counsel as follows:

I. INTRODUCTION

1. The Metropolitan Opera Association, Inc, located at Lincoln Center in the heart of midtown Manhattan, New York, New York, is the largest repertory opera house in the world. The Metropolitan Opera was opened in 1883 and is home to the Metropolitan Opera Company as well as the American Ballet Theatre. Collectively, the performances at The Met draw hundreds of thousands of visitors annually from around the world. The Metropolitan Opera is a tremendously successful organization and, as of December 2022, it maintained an endowment of $306 million.[1]

2. In the process of providing tickets to performances, selling merchandise and other goods and services to consumers, as well as collecting information from prospective and current employees (including independent contractors),[2] The Met collects a significant amount of personally identifiable information (hereinafter, the "PII") from current/former employees and consumers including, but not limited to: name, date of birth, financial account information, driver's license number, passport number, Social Security number, and/or tax identification number. Unfortunately, for over 49,000 of The Met's current/former employees and consumers, this PII was compromised in a significant data breach perpetrated by cybercriminals (the "Data Breach").

[1] Javier C. Hernandez, "*Pandemic Woes Lead Met Opera to Tap Endowment and Embrace New Work*," NEW YORK TIMES (ONLINE) (Dec. 26, 2022), at https://www.nytimes.com/2022/12/26/arts/music/metropolitan-opera-endowment-contemporary.html.

[2] Current and former employees includes family members of current and former employees who provided their PII or had their PII provided in order to receive benefits, such as health insurance.

3. On December 7, 2022, the New York Times reported that The Met's website and box office were out of commission for more than 30 hours due to a cyberattack.[3] The New York Times reported, "[i]t was not immediately clear who was responsible for the cyberattack … but the [Federal Bureau of Investigation] was aware of the situation."[4]

4. As it turns out, the cybercriminals, called the Snatch ransomware gang, not only disrupted The Met's website, online gift shop and box office, and payroll processing and key internal systems via ransomware applied to The Met's servers, but also exfiltrated sensitive data including the PII enumerated above. After The Met concluded an investigation into the Data Breach, which investigation was conducted by third party forensic specialists, The Met was able to ascertain that the cybercriminals did indeed steal the PII of Plaintiffs and the putative Class during the cybercriminals' unfettered access to The Met's computer systems during a two-month span (from September 30, 2022 through December 6, 2022). Thus, for over *two months*, The Met failed to detect an intruder with access to and possession of The Met's current/former employees' and consumers' highly sensitive data. It took a complete shutdown of The Met's website and box office for The Met to finally detect the presence of the intruder.

5. To compound matters, The Met's response to the Data Breach has been woefully insufficient: (1) The Met did not disclose the Data Breach to current/former employees and consumers and to relevant States' Attorneys General until May 3, 2023, nearly five months after The Met first detected the cyberattack on December 6, 2022; (2) The Met failed to disclose specifics of the cyberattack (*i.e.*, how it happened) as well as specific remedial measures taken to ensure the protection of the PII still in The Met's possession; and (3) The Met has offered victims

[3] Julia Jacobs, "*Cyberattack Take Down the Met Opera's Website and Box Office*," NEW YORK TIMES (ONLINE) (Dec. 7, 2022), at https://www.nytimes.com/2022/12/07/arts/met-opera-cyberattack-website.html.

[4] *Id.*

only 12 months of identity monitoring services when the impact of the theft of the PII at issue will ripple for many years, if not decades. Further, The Met's response to the Data Breach also allowed victims' injuries to snowball because of the reassurances The Met gave on their website on December 15, 2022, stating: "[b]ased upon our ongoing investigations into the recent cyberattack, we would like to reassure our customers that ticketing consumers data, including credit card information used when purchasing tickets, has not been stolen. We do not keep credit card information in the systems that were affected by the cyberattack." And yet, The Met offered no reassurances about any other type of data it collected, such as Social Security numbers belonging to former/current employees. The Met could have used the immediate window following the Data Breach to alert victims, but, instead, offered reassurances that were of no help to the Data Breach victims. On the contrary, these reassurances likely assuaged fears of victims that should not have been played down.

6. According to "RestorePrivacy," and as detailed more extensively below, the ransomware applied to The Met's servers was implemented and perpetrated by a notorious, Russian/Eastern European ransomware operation called Snatch.[5] Snatch added the information stolen from The Met by way of the Data Breach onto its website – meaning, the PII of Plaintiffs and the Class members is either currently (or was) for sale on the dark web.[6] The fact that this data was added to Snatch's website, and that The Met did nothing to notify consumers until two months after the data was posted is troubling. By dragging its feet, The Met allowed cybercriminals like Snatch to get a running start on harms to Plaintiffs and the Class members,

[5] Heinrich Long, "The Metropolitan Opera Admits Data Breach After Snatch Extortion," RESTORE PRIVACY (ONLINE) (May 4, 2023), at https://restoreprivacy.com/the-metropolitan-opera-admits-data-breach-after-snatch-extortion/.

[6] *Id.*

rather than accepting responsibility for The Met's defective cybersecurity apparatus. While The Met could have given Plaintiffs and Class members the ability to start taking action (like imposing credit freezes) to protect themselves, The Met made a conscious decision not to.

7. As such, Plaintiffs, on behalf of themselves and all others similarly situated, bring this Action for violations of state consumer protection laws, negligence, breach of implied contract and unjust enrichment, and seek restitution, actual damages, statutory damages, injunctive relief, disgorgement of profits and all other relief that this Court deems just and proper.

II. JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount of controversy exceeds the sum of $5,000,000 exclusive of interests and costs, there are more than 100 putative Class members, and minimal diversity exists because one or more putative Class members are citizens of a different state than Defendant. Additionally, the CAFA Home-State Exception does not apply because more than one third of putative Class members are from states other than New York.

9. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in New York, New York. Furthermore, Defendant intentionally availed itself of this jurisdiction by marketing, employing individuals, and providing services in New York, New York.

10. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant operates in this District and a substantial part of the events, acts and omissions giving rise to Plaintiffs' claims occurred in this District.

III. PARTIES

Plaintiff Rebecca Tuteur

11. Plaintiff Tuteur is a natural person and a resident of Forest Hills, New York. Plaintiff Tuteur's father was a Met employee and, as a result, Plaintiff Tuteur was on The Met's corporate health insurance plan and had her PII compromised in the Data Breach as alleged herein. Plaintiff Tuteur received a copy of the Data Breach Notification letter disseminated by Defendant.

12. As a result of Defendant's failure to protect her PII, Plaintiff Tuteur's name and Social Security number were compromised in the Data Breach and have since been fraudulently misused.

Plaintiff Anthony Viti

13. Plaintiff Viti is a natural person and a resident of Brooklyn, New York. Plaintiff Viti is a former employee of Defendant and had his PII compromised in the Data Breach as alleged herein. Plaintiff Viti received a copy of the Data Breach Notification letter disseminated by Defendant.

14. As a result of Defendant's failure to protect his PII, Plaintiff Viti's name, date of birth, financial account information, driver's license number, passport number, Social Security number, and tax identification number were compromised in the Data Breach.

Plaintiff Matthew Napoli

15. Plaintiff Napoli is a natural person and a resident of New York, New York. Plaintiff Napoli is a current employee of Defendant and had his PII compromised in the Data Breach as alleged herein. Plaintiff Napoli received a copy of the Data Breach Notification letter disseminated by Defendant.

16. As a result of Defendant's failure to protect his PII, Plaintiff Napoli's name, date of birth, financial account information, driver's license number, passport number, Social Security number, and tax identification number were compromised in the Data Breach.

Defendant Metropolitan Opera Association, Inc.

17. Defendant is a New York not-for-profit corporation with its principal place of business located in Lincoln Center, New York, New York. Defendant conducts a large part of its operations using, as its business name, the moniker "The Metropolitan Opera."

IV. FACTUAL ALLEGATIONS

Defendant's Business and Collection of PII

18. The Metropolitan Opera at Lincoln Center is an iconic New York venue where hundreds of thousands of visitors annually attend various performances and purchase related goods, merchandise and services. The Metropolitan Opera maintains a website, metopera.org, where consumers can shop for tickets and buy merchandise.

19. As of December of 2022, The Met maintains an endowment valued at $306 million and stages approximately 215 performances per season.[7] The Met has an annual budget of $312 million.[8]

20. In the course of its operations, The Met collects a significant amount of PII from current/former employees and consumers, including the following information: name, financial account information, tax identification number, Social Security number, payment card information and/or driver's license number. Plaintiffs and Class members needed to provide their PII to The

[7] Javier C. Hernandez, "*Pandemic Woes Lead Met Opera to Tap Endowment and Embrace New Work*," New York Times (Online) (Dec. 26, 2022) at https://www.nytimes.com/2022/12/26/arts/music/metropolitan-opera-endowment-contemporary.html.

[8] *Id.*

Met in conjunction with the services and employment that it offers. Plaintiffs and the Class willingly gave their PII to The Met with the understanding that The Met would protect that PII. Plaintiffs and Class members relied on the sophistication of The Met and its network to keep their PII confidential and securely maintained, to use this information for business and/or employment purposes only, and to only make authorized disclosures of this information. It is more than reasonable that Plaintiffs and Class members expected that their PII would be protected by The Met upon collection.

21. This information is collected pursuant to The Met's privacy policy, a document which is incorporated into each and every use of The Met's website. The Met's website states, "[b]y using this site, you agree to our Privacy Policy" on nearly every page of the website.[9]

22. In its privacy policy, Defendant acknowledges that it is the party responsible for the management of Plaintiffs' and Class members' PII, and promises not to disclose such information except for in limited circumstances, including to comply with applicable law and regulations, to cooperate with public and government authorities, to cooperate with law enforcement, for other legal reasons, and/or in connection with a sale or business transaction – none of which is applicable here."[10]

23. Consistent with Plaintiffs' expectations, as well as The Met's privacy policy, The Met collected a substantial amount of highly valuable PII. By collecting, using, and deriving a benefit from Plaintiffs' and Class members' PII, The Met assumed legal and equitable duties and

[9] THE METROPOLITAN OPERA, INTERNATIONAL PRIVACY POLICY, https://www.metopera.org/user-information/privacy-policy/#:~:text=We%20may%20use%20and%20disclose%20Other%20Information%20for%20any%20purpose,long%20as%20it%20is%20combined. (last visited July 31, 2023).
[10] *Id.*

knew or should have known that it was responsible for protecting Plaintiffs' and Class members' PII from unauthorized disclosure.

The Data Breach

24. On or about May 3, 2023, The Met notified states' Attorneys General of the Data Breach. This was done in part by disseminating a "Notice of Data Event" letter, which was posted to the Attorney General of Maine's website. That Notice of Data Event, dated May 3, 2023, states in relevant part:

> **Nature of the Data Event**
>
> On December 6, 2022, the Met identified suspicious activity related to its computer systems. The Met immediately took steps to secure their network and brought in a team of third-party information specialists to help the Met get its systems back up and running and to determine the nature and scope of the suspicious activity. Through an investigation conducted by third-party specialists, the Met learned that an unknown actor gained access to certain of their systems between September 30, 2022 and December 6, 2022 and accessed or took certain information from those systems. The Met completed a review of the contents of those files to determine what information was contained therein and to whom it related.
>
> The information that could have been subject to unauthorized access includes name, financial account information, tax identification number, Social Security number, payment card information, and driver's license number.
>
> …
>
> **Other Steps Taken and To Be Taken**
>
> Upon discovering the event, the Met moved quickly to investigate and respond to the incident, assess the security of the Met systems, and identify potentially affected individuals. Further, The Met notified federal law enforcement regarding the event. The Met is also working to implement additional safeguards and training to its employees. The Met is providing access to credit monitoring services for twelve (12) months, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.
>
> Additionally, the Met is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company

> and/or bank. The Met is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.
>
> The Met is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

25. The Met's response to the Data Breach has been woefully insufficient.

26. First, The Met did not disclose the Data Breach to current/former employees and consumers and to relevant States' Attorneys General until May 3, 2023, nearly five months after The Met first detected the cyberattack on December 6, 2022. This means that, for nearly five months, The Met could have alerted victims to the fact that their PII might have been compromised but failed to do so. Instead, The Met chose to sit on that information and allow valuable time to pass while Plaintiffs and members of the Class suffered the harms discussed herein.

27. Second, The Met has offered victims only 12 months of identity monitoring services when the impact of the theft of the PII at-issue ripples for decades. Although it is well-documented that the harms from identity theft can affect a person for a lifetime, The Met refuses to provide victims of the Data Breach with more than one year of monitoring services.

28. Finally, The Met failed to disclose specifics of the cyberattack (*i.e.*, how it happened) as well as the specific remedial measures, if any, taken to ensure the protection of the PII still in The Met's possession. This means that The Met either does not know how the cyberattack occurred and is not taking *any* remedial measures to rectify its deficient cybersecurity apparatus, or that The Met has chosen not to inform current/former employees and consumers of

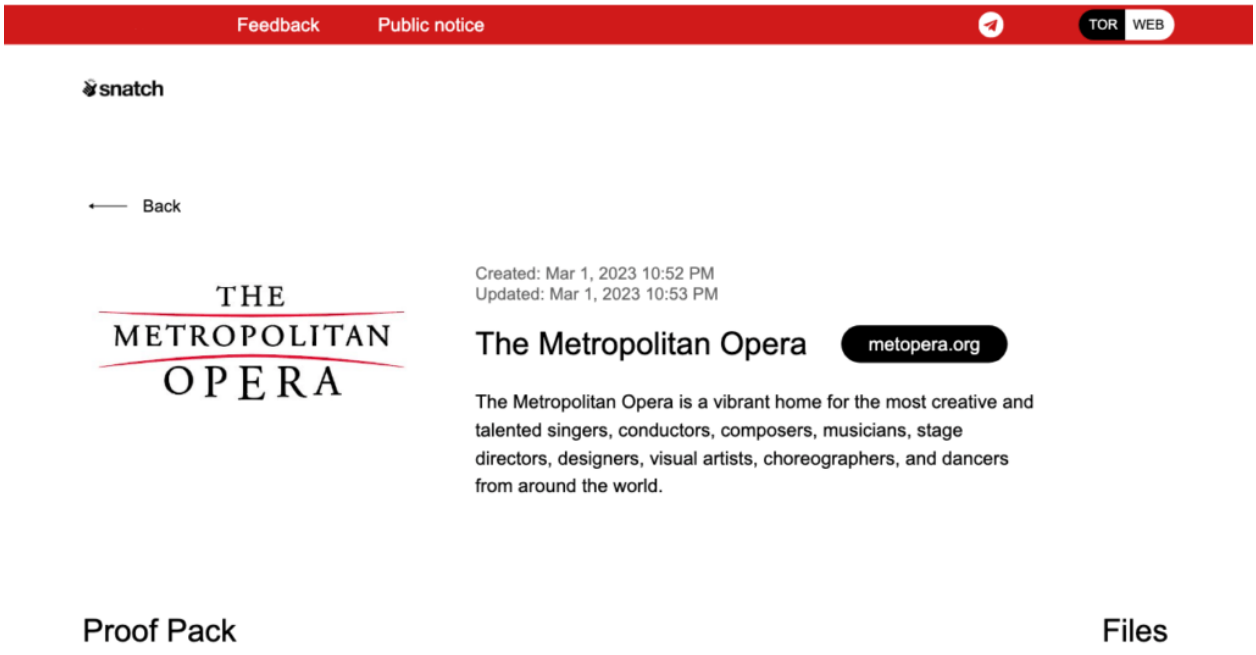
how their PII was stolen or how, if at all, their PII will be protected going forward. For victims of the Data Breach, all this information remains unclear.

29. But what is clear from the Notice is that cybercriminals did, in fact, access, view, and exfiltrate Plaintiffs' and Class members' PII during the period in which the cybercriminals had unfettered access to The Met's IT network, as that is the *modus operandi* of cybercriminals who commit such attacks. Indeed, according to "Restore Privacy", the Snatch ransomware gang assumed responsibility for the ransomware attack and subsequent exfiltration of data as alleged herein. Snatch is a well-known ransomware gang that lists over 70 victims on their dark web/extortion portal.[11] Some of the victims include Volvo Cars and McDonald's.

30. The strain of malware used by Snatch in the Data Breach "forces a restart on the victims' machine to [re]boot on Safe Mode, where security software does not run – [this] allow[s] the encryptor to execute unobstructed." And, because Snatch had unfettered access to The Met's systems from September 30, 2022 through December 6, 2022, Snatch had ample time to exfiltrate the amount of data that was stolen in the Data Breach.

31. The PII stolen in the Data Breach now is either for sale or was for sale through Snatch's extortion portal, as also evidenced by the fraudulent misuse of such information already experienced by Plaintiffs and Class members. An image of the portal to buy the data can be seen below:

[11] Heinrich Long, "The Metropolitan Opera Admits Data Breach After Snatch Extortion," RESTORE PRIVACY (ONLINE) (May 4, 2023), at https://restoreprivacy.com/the-metropolitan-opera-admits-data-breach-after-snatch-extortion/.



32. According to Restore Privacy, "[a]n interesting detail is that Snatch [removed] the Met entry from its extortion cite… [indicating] that the victim has paid the ransom or requested more time to negotiate."[12]

33. According to CyberWarzone, Snatch's *modus operandi* is as follows: "The Snatch Ransomware Gang employs a double extortion method, with payloads comprised of both ransomware and data stealing components. This allows the group to not only encrypt an organization's data, but also steal sensitive information, adding an additional layer of pressure on the victims. The group typically gains access to targets through automated, brute-force attacks against vulnerable applications." Notably, all of this information was omitted from the Notice of Data Breach.

[12] Heinrich Long, "The Metropolitan Opera Admits Data Breach After Snatch Extortion," RESTORE PRIVACY (ONLINE) (May 4, 2023), at https://restoreprivacy.com/the-metropolitan-opera-admits-data-breach-after-snatch-extortion/.

34. As such, The Met did not implement or maintain adequate measures to protect its current/former employees' and consumers' PII from attackers like Snatch.

35. On information and belief, the PII compromised in the files accessed by hackers was not encrypted. This can also be inferred given that Snatch was able to access the data that was listed as compromised in the Notice of Data Event and because Snatch was attempting to resell it (and there would be no purpose of buying the data in the event the PII was still encrypted).

36. Moreover, the removal of PII from The Met's system demonstrates that this cyberattack was targeted by Snatch due to The Met's status as a facility that houses sensitive PII. And, armed with this PII, data thieves, like Snatch, can commit a variety of crimes, including: opening new financial accounts in Class members' names, taking out loans in Class members' names, using Class members' information to obtain government benefits, filing fraudulent tax returns using Class members' tax identification information, obtaining driver's licenses in Class members' names but with a different photograph, and giving false information to police during an arrest. Indeed, some of these crimes have already been committed against Plaintiffs and Class members.

37. Due to The Met's flawed security measures and its incompetent response to the Data Breach, Plaintiffs and the Class members now face a present and substantial risk of fraud and identity theft and must deal with that threat forever.

38. Despite widespread knowledge of the dangers of identity theft and fraud associated with cyberattacks and unauthorized disclosure of PII, and despite The Met's generous operating budget and large endowment, The Met provided unreasonably deficient protections prior to the Data Breach, including but not limited to a lack of security measures for storing and handling PII and inadequate employee training regarding how to access, handle and safeguard this information.

39. The Met failed to adequately adopt and train its employees on even the most basic of information security protocols, including: storing, locking, encrypting and limiting access to current and former consumers and employees' highly sensitive PII; implementing guidelines for accessing, maintaining, and communicating sensitive PII; and protecting sensitive PII by implementing protocols on how to utilize such information.

40. The Met's failures caused the unpermitted disclosure of Plaintiffs' and Class members' PII to an unauthorized third-party cybercriminal and put Plaintiffs and Class members at serious, immediate, and continuous risk of identity theft and fraud.

41. The Data Breach that exposed Plaintiffs' and Class members' PII was caused by The Met's violation of its obligations to abide by best practices and industry standards concerning its information security practices and processes.

42. The Met failed to comply with security standards or to implement security measures that could have prevented or mitigated the Data Breach.

43. The Met failed to ensure that all personnel with access to its current/former employees' and consumers' PII were properly trained in retrieving, handling, using and distributing sensitive information. Further, there have been no assurances offered by The Met that all personal data or copies of the PII at issue was either recovered, destroyed, or otherwise protected by an enhanced data security protection apparatus.

The Breach Was Foreseeable

44. The Met had weighty obligations created by industry standards, common law, and its own promises and representations made to Plaintiffs and Class members to keep their PII confidential and to protect it from unauthorized access and disclosure.

45. Plaintiffs and Class members provided their PII to The Met with the reasonable expectation and mutual understanding that The Met would comply with its obligations to keep such information confidential and secure from unauthorized access.

46. The Met's data security obligations were particularly acute given the substantial increase in ransomware attacks and/or data breaches in various industries preceding the date of the Data Breach.

47. The Met was aware of the risk of data breaches because such breaches have dominated the headlines in recent years.

48. Cyberattacks have become so notorious that the Federal Bureau of Investigation and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.

49. PII is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used in a variety of unlawful manners. PII can be used to distinguish, identify or trace an individual's identity. This can be accomplished alone or in combination with other personal or identifying information that is connected or linked to an individual, such as the information compromised in the Data Breach.

50. Given the nature of the Data Breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of different ways.

51. Cybercriminals who possess the Class members' PII can readily obtain Class members' tax returns or open fraudulent credit card or other types of accounts in the Class members' names.

52. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in The Met's industry, including to The Met.

53. Indeed, this specific Data Breach was foreseeable. The Met was cognizant of data breaches because of how common and high-profile data breaches have become with respect to consumer-facing businesses and businesses that employ thousands of people, as The Met does.

Defendant Failed to Follow FTC Guidelines and Industry Standards

54. Experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the data which they collect and maintain. The reason this data is so valuable is because it contains PII, which can be sold and weaponized for purposes of committing various identity theft-related crimes. It is well-known that, because of the value of this data and PII, businesses that collect, store, maintain, and otherwise utilize or profit from PII must take necessary cybersecurity safeguards to ensure that the data they possess is adequately protected.

55. Government agencies also highlight the importance of cybersecurity practices. For example, the Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

56. According to the FTC, the need for data security should be factored into all business decision-making.

57. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.

58. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

59. The guidelines also recommend that businesses use an intrusion detection system to detect and expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

60. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

61. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, in some cases treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further explicate and clarify the measures businesses must take to meet their data security obligations.

62. The Met failed to properly implement some or all of these (and other) basic data security practices.

63. The Met's failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

64. The Met was at all times fully aware of its obligation to protect the PII of its current/former employees and consumers. The Met was also aware of the significant repercussions that would result from its failure to do so.

65. Experts studying cyber security routinely identify consumer-facing businesses as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

66. Several best practices have been identified that, at a minimum, should be implemented by consumer goods and services providers and employers such as The Met, including but not limited to: educating all employees about cyber security; requiring strong passwords; maintaining multi-layer security, including firewalls, anti-virus, and anti-malware software; utilizing encryption; making data unreadable without a key; implementing multi-factor authentication; backing up data; and limiting which particular employees can access sensitive data.

67. Other best cybersecurity practices that are standard in the industry include installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; and training staff regarding critical points.

68. These foregoing frameworks are existing and applicable industry standards. The Met failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

The Met's Breach of Its Obligations

69. The Met breached its obligations to Plaintiffs and Class members and was otherwise negligent and/or reckless because it failed to properly maintain and safeguard its computer systems, network and data. In addition to its obligations under federal and state law, The Met owed a duty to Plaintiffs and the Class members to exercise reasonable care when obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from

being compromised, lost, stolen, accessed or misused by unauthorized persons. The Met owed a duty to Plaintiffs and Class members to provide reasonable security, including complying with industry standards and requirements, training for its staff and ensuring that its computer systems, networks, and protocols adequately protected the PII of Plaintiffs and the Class members.

70. The Met's wrongful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect current/former employees' and consumers' PII;

c. Failing to properly monitor its own data security systems for existing intrusions, brute-force attempts and clearing of event logs;

d. Failing to apply all available and necessary security updates;

e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

f. Failing to practice the principle of least-privilege and maintain credential hygiene; and failing to avoid the use of domain-wide, admin-level service accounts;

g. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords; and

h. Failing to properly train and supervise employees in the proper handling of inbound emails.

71. As the result of allowing its computer systems to fall into dire need of security upgrading and its inadequate procedures for handling cybersecurity threats, The Met negligently and wrongfully failed to safeguard Plaintiffs' and Class members' PII.

72. Accordingly, as further detailed herein, Plaintiffs and Class members now face a substantial, increased, and immediate risk of fraud, identity theft, and the disclosure of their most sensitive and deeply personal information.

Data Breaches Are Disruptive and Harm Victims

73. The United States Government Accountability Office ("GAO") released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

74. That is because all victims of a data breach may be exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it because there is (unfortunately) a market for personally identifiable information, like the PII compromised by the Data Breach.

75. Cybercriminals do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate individual pieces of data an identity thief obtains regarding a person, the easier it is for that thief to take on the victim's identity, or otherwise harass or track the victim.

76. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information regarding a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

77. The type of information compromised in this Data Breach is even worse than merely a name and date of birth. A stolen Social Security number is a skeleton key to the victim's identity – and, therefore, the type of data that cyberthieves seek. Identity thieves can use a Social Security number for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, fraudulently obtaining a job, fraudulently renting a house, or filing a false police report. The Data Breach also exposed driver's license numbers and tax identification information, which can result in fake driver's licenses being obtained by thieves, as well as the filing of false tax returns or stealing a victim's tax refund.

78. Because of the threat of these harms, the FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and potentially obtaining an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

79. Theft of PII is gravely serious. PII is an extremely valuable property right.

80. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates that PII has considerable market value.

81. According to the GAO:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

82. Private information, such as the PII compromised herein, is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. The private information of consumers remains of high value to criminals, as evidenced by the prices paid through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, private information (inclusive of a Social Security number) can be sold at a price from $40 to $200, and bank details have a price range of $50 to $200. Experian reports that a stolen credit card or debit card number can sell between $5 to $110 on the dark web. Clearly, all of this data has real value – which is why it was targeted and stolen in the first place.

83. Because of the value of the PII compromised in the Data Breach, there is a strong probability that entire batches of information stolen in the Data Breach have been dumped on the black market, as that is the *modus operandi* of cybercriminals who perpetrate data breaches, while other batches have yet to be dumped on the black market, meaning Plaintiffs and Class members are at a substantial imminent risk of injury including an increased risk of fraud and identity theft for many years into the future.

84. Thus, Plaintiffs and Class members must vigilantly monitor their financial accounts and other indices of identity theft (*i.e.*, the mail, email, etc.) for many years to come.

Harm to Plaintiffs

85. On or about May 3, 2023, Plaintiffs received notice from The Met that their PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiffs' PII was compromised as a result of the Data Breach.

86. As a result of the Data Breach, Plaintiffs have commenced making reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data

Breach, and reviewing reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiffs have already spent multiple hours dealing with the Data Breach, valuable time Plaintiffs otherwise would have spent on other activities.

87. Plaintiffs suffered actual injury from having their PII compromised as a result of the Data Breach including, but not limited to (a) actual misuse of their compromised PII; (b) damage to and diminution in the value of their PII, a form of property that The Met obtained from Plaintiffs; (c) violation of their privacy, including the compromise of highly sensitive PII such as, for example, their Social Security numbers in combination with their names other private information; (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud; and (e) actual and potential loss of time, as each of the Plaintiffs has spent multiple hours dealing with the repercussions of the Data Breach, due to time spent mitigating the actual and potential harms caused by the Data Breach.

88. In fact, Plaintiff Tuteur has, unfortunately, already experienced the fraudulent misuse of her PII compromised in the Data Breach through the opening of fraudulent bank accounts, credit cards, and phone plans in her name. Specifically, a Bank of America account was opened and fake checks were deposited in her name on or around February 20, 2023. On or around February 21, 2023, a Verizon account and mobile phone line were opened in her name without her knowledge or authorization. A credit card was also applied for in her name on or around February 22, 2023, without her knowledge or authorization. On or around February 22, 2023, a Discover credit card was also opened in her name without her knowledge or authorization. Around this same time, there was an unauthorized attempt through the United States Postal Service to change her permanent mailing address. In or around early March, fraudulent requests for her tax information were made with the Internal Revenue Service without her knowledge or authorization. On or

around March 23, 2023, an American Express card was opened in her name without her knowledge or authorization. On or around March 31, 2023, a Go2Bank debit card was opened in her name without her knowledge or authorization.

89. As evidenced by the misuse that has already occurred in Plaintiff Tuteur's case, all of which occurred soon after the Data Breach, it is clear that Plaintiffs' and Class members' PII is already in the hands of and being misused by criminals due to the highly confidential nature of this PII and its significant value to hackers and criminals, as well as the obvious fact that this cyberattack would not have been executed without some motivation to steal it for nefarious purposes. Unfortunately for the victims of the Data Breach, the cybercriminals executed a sophisticated attack on The Met for which The Met lacked minimal and adequate protections to avoid this PII being exfiltrated (like adequately encrypting the data, among numerous others available safeguards).

90. As such, and because of the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiffs are at a present, immediate and substantial risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ALLEGATIONS

91. This Action is properly maintainable as a Class Action pursuant to Federal Rule of Civil Procedure 23, *et seq.* Plaintiffs bring this Action on behalf of themselves and all other similarly situated persons for the following Class defined as:

> **Class Definition.** All individuals and entities residing in the United States whose PII was compromised in the Data Breach announced by Defendant in May of 2023, including all who were sent a notice of the Data Breach.

(collectively, the "Class").

92. Excluded from the Class are Defendant and Defendant's subsidiaries, affiliates, officers and directors, and any entity in which the Defendant has a controlling interest; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

93. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

94. **Numerosity**. Defendant reports that the Data Breach compromised PII of 49,000+ current and former employees and consumers. Therefore, the members of the Class are so numerous that joinder of all members is impractical.

95. **Commonality**. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost or disclosed Plaintiffs' and Class members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Plaintiffs and Class members to safeguard their PII;

f. Whether Defendant breached its duty to Plaintiffs and Class members to safeguard their PII;

g. Whether computer hackers obtained Plaintiffs' and Class members' PII in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiffs and Class members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant breached an implied contract with Plaintiffs and Class Members;

j. Whether Defendant's acts, inactions, and practices complained of herein amount to violations of N.Y. Gen. Bus. Law 349 and/or common law negligence, and whether Defendant has been unjustly enriched;

k. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

l. Whether Plaintiffs and Class members are entitled to damages, civil penalties, punitive damages, equitable relief and/or injunctive relief.

96. **Typicality**. Plaintiffs' claims are typical of those of other Class members because Plaintiffs' PII, like that of every other Class member, was compromised by the Data Breach. Further, Plaintiffs, like all Class members, were injured by Defendant's uniform conduct. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of other Class members arise from the same operative facts and are based on the same legal theories.

97. **Adequacy of Representation**. Plaintiffs will fairly and adequately represent and protect the interests of the Class in that they have no disabling or disqualifying conflicts of interest that would be antagonistic to those of the other members of the Class. The damages and infringement of rights Plaintiffs suffered are typical of the other Class members, and Plaintiffs seek no relief that is antagonistic or adverse to the members of the Class. Plaintiffs have retained counsel experienced in complex class action litigation, including, but not limited to, data privacy class action litigation, and Plaintiffs intend to prosecute this action vigorously.

98. **Superiority of Class Action**. A class action is superior to other available methods for the fair and efficient adjudication of this controversy, as the pursuit of numerous individual lawsuits would not be economically feasible for individual Class members, and certification as a class action will preserve judicial resources by allowing the Class's common issues to be adjudicated in a single forum, avoiding the need for duplicative hearings and discovery in individual actions that are based upon an identical set of facts. Without a class action, it is likely that many members of the Class will remain unaware of the claims they may possess.

99. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws and the ascertainable identities of Class members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

100. Adequate notice can be given to Class members directly using information maintained in Defendant's records.

101. **Predominance**. The issues in this action are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Defendant has engaged in a common course of conduct toward Plaintiffs and Class members in that all of the victims of the Data Breach had their PII stored on the same computer systems and was unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendant's conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these issues in a single action has important and desirable advantages of judicial economy.

102. This proposed class action does not present any unique management difficulties.

FIRST CAUSE OF ACTION

VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW SECTION 349

103. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

104. New York General Business Law Section 349 ("New York Gen. Bus. Law 349") prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

105. Defendant is a business as defined by the statue.

106. Plaintiffs and Class members are consumers as defined by the statute.

107. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of New York Gen. Bus. Law 349. The conduct alleged is a "business practice" as defined by the statute, and the deception occurred in New York state.

108. Defendant engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class members' PII, which was a proximate and direct cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents involving other organizations, which was a direct and proximate cause of the Data Breach;

c. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class members' PII, including by implementing and maintaining reasonable security measures;

d. Failing to timely and adequately notify Plaintiffs and Class members of the Data Breach;

e. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' PII; and

f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

109. Defendant's representations and omissions regarding data security were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of PII.

110. Defendant acted intentionally and knowingly to violate New York's General Business Law, and recklessly disregarded Plaintiffs' and Class members' rights.

111. As a direct and proximate result of Defendant's deceptive and unlawful acts and practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; and the other harms detailed herein.

112. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large. Defendant's violations of the statute have had an impact on the public, including the people of New York, because thousands of New Yorkers had their PII stored in The Met's electronic database, many of whom have been impacted by the Data Breach.

113. The above deceptive and unlawful practices and acts by Defendant caused substantial injury to Plaintiffs and Class members that they could not reasonably avoid.

114. As such, Plaintiffs and the Class members seek statutory damages in the maximum amount allowed per Class member, or, $50 for each of the more than 49,000 victims of the Data Breach. Additionally, Plaintiffs and the Class members seek injunctive relief necessary to enjoin further violations and recover costs of this action, including reasonable attorneys' fees and other costs.

SECOND CAUSE OF ACTION

NEGLIGENCE

115. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

116. Defendant required Plaintiffs and Class members to submit non-public personal information in order to obtain employment and/or purchase goods and services.

117. Plaintiffs and Class members are individuals who provided certain PII to Defendant including the PII described above.

118. Defendant had full knowledge of the sensitivity of the PII to which it was entrusted and the types of harm that Plaintiffs and Class members could and would suffer if the information were wrongfully disclosed.

119. Defendant had a duty to Plaintiffs and each Class member to exercise reasonable care in holding, safeguarding and protecting that information.

120. Plaintiffs and Class members were the foreseeable victims of any inadequate safety and security practices.

121. Plaintiffs and Class members had no ability to protect their data in Defendant's possession.

122. By collecting and storing this data in its computer property, and by sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its technology — and Plaintiffs' and the Class members' PII held within it — to prevent disclosure of the information and to safeguard the information from theft.

123. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a data breach.

124. Defendant owed a duty of care to safeguard the PII of Plaintiffs and Class members in its custody. This duty of care arises because Defendant knew of a foreseeable risk to the data security systems it used. Defendant knew of this foreseeable risk because of the explosion of data breach incidents detailed above and in an avalanche of media reports in recent years. Despite its knowledge of this foreseeable risk, Defendant failed to implement reasonable security measures.

125. Defendant owed a duty of care to Plaintiffs and Class members to provide data security consistent with industry standards and other requirements detailed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

126. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class members from a data breach.

127. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

128. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

129. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect the Plaintiffs' and Class members' PII.

130. The specific negligent acts and omissions committed by Defendant includes, but are not limited to, the following:

a. Failing to adopt, implement and maintain adequate security measures and practices to safeguard Plaintiffs' and Class members' PII;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its network system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Plaintiffs' and Class members' PII;

e. Failing to detect in a timely manner that Plaintiffs' and Class members' PII had been compromised;

f. Failing to timely notify Plaintiffs and Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

131. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiffs' and Class members' PII would result in injury to Plaintiffs and Class members.

132. Further, the Data Breach was reasonably foreseeable given the known high frequency of hacking incidents, cyberattacks, and data breaches in the consumer goods and services industry.

133. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs' and Class members' PII would result in one or more types of injuries to Plaintiffs and Class members.

134. Plaintiffs and Class members were harmed as a result of Defendant's negligence in the manner alleged herein. Plaintiffs and Class members have suffered injury and are entitled to damages in an amount to be proven at trial.

135. In addition to monetary relief, Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide a lifetime of credit monitoring and identity theft insurance to Plaintiffs and Class members.

THIRD CAUSE OF ACTION

BREACH OF CONTRACT

136. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

137. Plaintiffs and Class members entered into a valid and enforceable contract through which they paid money to Defendant in exchange for services, or, in the case of current and former employees of Defendant, they provided services to Defendant in exchange for certain compensation. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiffs' and Class members' PII.

138. Defendant's Privacy Policy memorialized the rights and obligations of Defendant and its current and former employees and customers. This document was provided to Plaintiffs and Class members in a manner in which it became part of the parties' agreement.

139. In the Privacy Policy, Defendant commits to protecting the privacy and security of private information and promises to never share Plaintiffs' and Class members' PII except under certain limited circumstances.

140. Plaintiffs and Class members fully performed their obligations under their contracts with Defendant.

141. However, Defendant did not secure, safeguard, and/or keep private Plaintiffs' and Class members' PII, and therefore Defendant breached its contracts with Plaintiffs and Class members.

142. Defendant allowed third parties to access, copy, and/or exfiltrate Plaintiffs' and Class members' PII without permission. Therefore, Defendant breached the Privacy Policy with Plaintiffs and Class members.

143. As a result, Plaintiffs and Class members have been harmed, damaged, and/or injured as described herein, including in Defendant's failure to fully perform its part of the bargain with Plaintiffs and Class members.

144. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members suffered and will continue to suffer damages in an amount to be proven at trial.

145. In addition to monetary relief, Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class members.

FOURTH CAUSE OF ACTION

BREACH OF IMPLIED CONTRACT

146. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

147. This cause of action is brought alternatively to Plaintiffs' claim for breach of contract.

148. Defendant provides entertainment services and/or employment to Plaintiffs and Class members. Defendant formed an implied contract with Plaintiffs and Class members through their collective conduct.

149. Through the Defendant's provision of goods and services, and its provision of employment opportunities, it knew or should have known that it must protect Plaintiffs' and Class members' confidential PII in accordance with Defendant's stated policies, practices and the applicable law.

150. As consideration, Plaintiffs and Class members turned over valuable PII (as well as either money or employment services) in exchange for either entertainment services or for employment.

151. Defendant accepted possession of Plaintiffs' and Class members' PII for the purpose of providing goods and services to Plaintiffs and the Class members, or for the purpose of obtaining Plaintiffs' and Class members' services as employees. In delivering their PII to Defendant, Plaintiffs and the Class members intended and understood that Defendant would adequately safeguard the PII as part of the provision or receipt of those goods or services.

152. Defendant's implied promises to Plaintiffs and Class members include, but are not limited to: (1) taking steps to ensure that anyone who is granted access to PII also protects the

confidentiality of that data; (2) taking steps to ensure that the PII placed in control of Defendant's employees is restricted and limited only to achieve authorized business purposes; (3) restricting access to employees and/or agents who are qualified and trained; (4) designing and implementing appropriate retention policies to protect PII; (5) applying or requiring proper encryption and/or the separation of different data sets; (6) implementing multifactor authentication for access; and (7) taking other steps to protected against foreseeable breaches.

153. Plaintiffs and Class members would not have entrusted their PII to Defendant in the absence of such an implied contract.

154. Defendant violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class members' PII.

155. Plaintiffs and Class members have been damaged by Defendant's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein. Plaintiffs seek damages in an amount to be proven at trial.

156. In addition to monetary relief, Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide a lifetime of credit monitoring and identity theft insurance to Plaintiffs and the Class members.

FIFTH CAUSE OF ACTION

UNJUST ENRICHMENT

157. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

158. This Cause of Action is pled and offered in the alternative to Plaintiffs' Third and Fourth Causes of Action.

159. Plaintiffs and Class members conferred a benefit upon Defendant with their money and/or labor services. Specifically, they either worked as employees and/or purchased goods and services from Defendant. In doing so, they also provided Defendant with their PII. In exchange, Plaintiffs and Class members should have received from Defendant the employment, and/or goods and services that were the subject of their respective transactions and should have had their PII protected with adequate data security.

160. Defendant knew that Plaintiffs and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiffs and Class members for business purposes.

161. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own operating profits at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures. Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own operating profits over the requisite security.

162. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class members, because Defendant failed to implement appropriate data management and security measures.

163. Defendant failed to secure Plaintiffs' and Class members' PII and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

164. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices detailed herein.

165. Had Plaintiffs and Class members known that Defendant had not reasonably secured their PII, they would not have agreed to provide their PII to Defendant.

166. Plaintiffs and Class members have no adequate remedy at law.

167. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the value and opportunity in respect of how their PII is used; (c) the compromise, publication, and/or theft of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (e) lost opportunity costs associated with the time and efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued immediate risk to their PII, which remains in Defendant's possession and is subject to yet further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in its continued possession; and/or (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class members.

168. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members have suffered and will continue to suffer these and other forms of injury and/or harm.

169. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services and goods, or (in the case of current/former

employees) the full value of the services such current/former employees provided to Defendant after taking into account that their PII was not protected from loss in the manner that Defendant has represented.

SIXTH CAUSE OF ACTION

DECLARATORY JUDGMENT

170. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

171. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state laws and regulations described in this Complaint.

172. Defendant owes a duty of care to Plaintiffs and Class members, which required it to adequately secure Plaintiffs' and Class members' PII.

173. Defendant still possesses PII regarding Plaintiffs and Class members.

174. Plaintiffs allege that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and the risk remains that further compromises of their PII will occur in the future.

175. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure its victims' PII and to timely notify victims of a data breach;

b. Defendant's existing data security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect PII; and

c. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure victims' PII.

176. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with legal and industry standards to protect victims' PII, including the following:

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

ii. ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

iii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iv. auditing, testing, and training its security personnel regarding any new or modified procedures;

v. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

vi. conducting regular database scanning and security checks;

vii. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

viii. meaningfully educating its users about the threats they face with regard to the security of their PII as well as the steps Defendant's customers, and employees should take to protect themselves.

177. If an injunction is not issued, Plaintiffs and Class members will suffer irreparable injury and will lack adequate legal remedy to prevent another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach of Defendant's systems occurs, Plaintiffs and Class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

178. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiffs and Class members will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

179. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at

Defendant, thus preventing future injury to Plaintiffs and other customers whose PII would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on their own behalf and on behalf of all others similarly situated, pray for relief as follows:

A. For an Order certifying this case as a class action;

B. For an award of restitution, actual damages, compensatory damages, statutory damages, nominal damages and statutory penalties, in an amount to be determined, as allowable by law;

C. For an award of equitable and injunctive relief;

D. For injunctive and other equitable relief to ensure the protection of the sensitive information of Plaintiffs and the Class which remains in Defendant's possession;

E. For an award of attorneys' fees and costs;

F. For pre- and post-judgment interest on any amounts awarded; and

G. For such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMAND

180. Plaintiffs hereby demand a trial by jury of all claims so triable.

DATED: August 3, 2023

Respectfully submitted,

/s/ *Israel David*
Israel David
Blake Hunter Yagman
Madeline Sheffield
ISRAEL DAVID LLC
17 State Street, Suite 4010
New York, New York 10004
Tel.: 212-739-0622
Fax: 212-739-0628
Email: *israel.david@davidllc.com*
blake.yagman@davidllc.com
madeline.sheffield@davidllc.com

Interim Lead Class Counsel

Mason A. Barney
Tyler J. Bean
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel. (212) 532-1091
Email: *mbarney@sirillp.com*
tbean@sirillp.com

Attorneys for Plaintiff Rebecca Tuteur